Il trojan di stato tedesco - sfide tra la legge e la tecnologia

Il trojan "di stato" tedesco - sfide tra la legge e la tecnologia

Scritto da Wiebke Abel e Burkhard Schafer, University of Edinburgh

Lunedì 02 Marzo 2009 17:39

Traduzione di The German "Federal Trojan" - challenges between law and technology, a cura di Teutas.

Introduzione. Il Consiglio dell'Unione europea ha recentemente raccomandato che gli Stati membri si adoperino per l'esame in remoto dei computer di sospetti, se questo è previsto dal diritto nazionale (Consiglio dell'Unione europea, 2008). Questo articolo analizza le questioni alle quali probabilmente gli Stati membri dovranno far fronte se decideranno di regolamentare questo nuovo tipo di strumento investigativo, attingendo dalle esperienze che la Germania ha fatto nel suo tentativo di regolamentare l'uso di strumenti di "remote forensics" da parte dei soggetti che devono far rispettare la legge.

I recenti sviluppi nell' intelligenza artificiale e nell'informatica hanno influenzato il modo in cui le forze di polizia e gli organismi preposti all'applicazione della legge sono operativi e la lotta contro la criminalità. L'evoluzione di tecnologie autonome e semi-autonome ha portato all'adozione di nuovi metodi di indagine e di raccolta delle prove.
Questa nuova generazione di tecnologie, come agenti software e trojan, ha caratteristiche uniche, che la distingue dalle tecnologie esistenti attualmente utilizzate nelle indagini. Durante le indagini, queste tecnologie sono in grado di andare oltre la semplice esecuzione di comandi di operatore, e agire in modo autonomo. La loro capacità decisionale autonoma consente loro di sostituire almeno alcune delle funzioni precedentemente svolte da personale umano, e senza la supervisione diretta di un controllore umano. Ciò solleva la questione se le norme che conferiscono diritti ai funzionari umani possono essere applicate per analogia agli agenti software, e se le norme che hanno lo scopo di limitare le interferenze della polizia sui diritti del cittadino possano essere aggirate utilizzando tecnologia (Schafer, 2006).

2. Trojan "di stato" e altri strumenti d'indagine

Il trojan "di stato" tedesco

Nel corso di una recente indagine nei confronti di un sospetto in un caso di terrorismo, i procuratori penali tedeschi hanno ipotizzato che le informazioni essenziali per l'inchiesta avrebbero potuto essere memorizzate sul computer del sospetto (Hornung, 2007). Pertanto, il procuratore generale ha chiesto al giudice un mandato per ispezionare segretamente il computer del sospetto. La domanda richiedeva il permesso di esaminare i dati memorizzati sul disco rigido e la memoria del computer. A tale scopo, doveva essere caricato sul computer dell'indagato un programma software specificamente progettato senza destare sospetti. Questo programma avrebbe copiato tutti i dati memorizzati sul computer e quindi li avrebbe trasferiti presso l'autorità inquirente per la valutazione. Oltre che per i file memorizzati sul computer, l'accesso è stato chiesto per il traffico e-mail e per le informazioni sui siti web visitati (Leipold, 2007).
Per preparare il terreno per l'analisi che faremo nella seconda parte di questo articolo, diamo alcune indicazioni sul modo in cui la tecnologia è in grado di lavorare. Ci sono pochi dati disponibili al momento circa l'esatta natura degli "strumenti forensi in remoto " (remote forensics tools - remote forensics software RFS-). Questo saggio si focalizza sull'uso di software che condivide caratteristiche essenziali col "malware", in particolare i virus e trojan. Entrambi possono essere utilizzati per l'accesso e l'estrazione di dati personali, e quindi sono adatti per la raccolta dei dati dalle autorità di polizia. Il vantaggio di utilizzare queste tecnologie è che sono progettati per confondersi come qualcosa di innocuo, quando in realtà includono un codice "maligno" o "nocivo" e, quindi ingannano l'indagato che li installa. Tuttavia, come con i loro omologhi, i trojan della polizia richiedono la cooperazione inconsapevole del destinatario. Ciò può avvenire attraverso l'apertura di un messaggio di posta elettronica, per esempio una e-mail che si presume provenga da un organismo statale accreditato, come il consiglio comunale o il dipartimento per le pensioni. Per ovvie ragioni, gli investigatori della polizia avrebbero poche difficoltà a generare messaggi di posta elettronica che non possono essere distinti dai filtri anti-spam e software analoghi rispetto ad informazioni vere provenienti da altre autorità pubbliche; queste autorità pubbliche possono essere la fonte del messaggio, che porta il trojan come una carico, da parte della polizia. Potrebbe anche non essere necessario falsificare l'indirizzo del mittente e altri dati identificativi incorporati in un messaggio email.

2.2 Un singolo caso?

L'uso del trojan o altri software per scopi di indagine da parte delle forze dell'ordine individua un approccio del tutto nuovo in Germania, e mostreremo più avanti in questo documento come questo provoca problemi giuridici e tecnici. Altri paesi hanno valutato la necessità di nuovi strumenti d'indagine analoghi. Tuttavia, non è noto se questi paesi stiano utilizzando tecnologie simili o seguendo un approccio diverso. Per una discussione sulla regolamentazione di queste tecnologie, è importante stabilire se l'uso di strumenti di indagine RFS a scopi investigativi sia un fenomeno internazionale. Ai fini del presente articolo, si analizza brevemente la situazione in altri due paesi, gli Stati Uniti e l' Austria. In entrambi i paesi, vi è stata una recente discussione sull'uso e la progettazione di nuovi strumenti d'indagine basati su software.

Negli Stati Uniti circolano dal 1999 (Poulsen, 2007) strumenti d'indagine basati su software, utilizzati dall' FBI, finalizzati a verificare la comunicazione attraverso le tecnologie collegate ad Internet. Il primo strumento progettato e utilizzato dalle agenzie di intelligence e della cui esistenza è stata data notizia, è un sistema chiamato Carnivore. Questo strumento di sorveglianza è installato nell'hardware tra il computer dell'indagato e Internet, quindi, di solito sul computer del provider di servizi Internet (ISP) dell'indagato. Quindi cattura tutte le informazioni scambiate tra l'indagato e il computer dell'ISP, come le email e gli indirizzi IP: pertanto, presumibilmente, trasmettendo solo informazioni su persone o indirizzi e-mail specificate nel mandato che consente l'uso dello strumento (Forno, 2000) .

Carnivore è stato sostituito da un altro software chiamato Magic Lantern. Questo strumento è più avanzato, nella misura in cui è possibile installarlo direttamente sul computer dell'indagato. Pertanto, nessun terzo è coinvolto nel processo di sorveglianza. Il software è incorporato in un virus o Trojan, e per infiltrarsi nel sistema dell'indagato vengono utilizzati allegati ingannevoli di posta elettronica o le vulnerabilità nei sistemi operativi. È stato progettato per monitorare i tasti digitati dal sospetto, che possono poi essere analizzati dalle autorità per estrarre le password (Poulsen, 2007).

Il più recente software di indagine e strumento di sorveglianza che è stato sviluppato negli Stati Uniti per l'utilizzo da parte delle autorità è il Computer e Internet Protocol Address Verifier (CIPAV). Questo software è, ancora una volta, installato direttamente sul computer del sospetto. E' in grado di catturare una serie di informazioni, come ad esempio indirizzo IP, indirizzi Ethernet MAC, l'elenco delle porte TCP e UDP aperte, i programmi in esecuzione, il tipo di sistema operativo e il numero di serie, il browser predefinito, l' utente registrato per il sistema operativo e l'ultima URL visitata (Poulsen, 2008). Offre quindi l'accesso in tempo reale al disco rigido del computer di destinazione. Inoltre, dopo aver catturato e trasferito tali informazioni, il CIPAV rimane attivo sotto forma di un "registro delle telefonate fatte" per 60 giorni, e monitora l'uso di Internet (Poulsen, 2007).

Tutti e tre gli strumenti hanno in comune il fatto che monitorano nascostamente i computer dei sospetti. Le persone tenute sotto controllo potrebbero non scoprire mai che questi strumenti sono stati utilizzati per raccogliere informazioni su di essi.

La misura in cui questi strumenti sono stati e vengono usati è difficile da determinare. Le informazioni relative sono "sensibili" e solo in rare occasioni, rese pubbliche. Vi è un caso riferito dove il software CIPAV è stato utilizzato per controllare una persona sospettata di minacce di "bombardamento email" contro una scuola superiore di Washington nel 2007 (Poulsen, 2007).

L'Austria ha un approccio diverso al tema delle operazioni di ricerca online sui computer dei sospetti. Attualmente si sta valutando teoricamente se la ricerca con RFS su un computer sospetto sia legale ed auspicabile. Un gruppo di lavoro del Ministero federale per gli affari interni e giustizia, ha compilato e di recente pubblicato una relazione su questo tema, raccomandando che le operazioni di ricerca online utilizzando un RFS dovrebbero essere generalmente ammesse (Bundesministerielle Arbeitsgruppe, 2008). Tuttavia, dovrebbero essere usate solo nei casi in cui è prevista una pena di 10 anni di carcere o più ed un giudice abbia emesso un mandato che esplicitamente ammetta l'uso di tale strumento. Inoltre, l'indagato deve essere gravemente sospettato (Tagesspiegel, 2007). Viene inoltre anticipato che verrà approvata a breve una legge che sia in linea con queste linee guida e che ammetta la ricerca on line usando uno strumento RFS.

La breve analisi di cui sopra mostra che entrambi i paesi stanno introducendo o stanno già usando strumenti d'indagine che sono stati progettati per la ricerca a distanza su un computer, per copiare i dati e, successivamente, per trasmetterli all'operatore. Pertanto, entrambi i paesi sono ugualmente interessati a progettare strumenti RFS, come i Trojan, per l'uso da parte delle forze dell'ordine. Ciò dimostra che il "trojan tedesco" non è un caso isolato, ma che questo è un fenomeno internazionale.

3. Remote Forensic Software strumenti d'indagine - Caratteristiche e sfide

Gli strumenti RFS, come i trojan sono dotati di molte caratteristiche uniche. In primo luogo, questi nuovi strumenti di indagine sono mobili. Mobile, in questo contesto, significa che essi possono muoversi tra le varie macchine e

architetture, utilizzando Internet come mezzi di trasporto (D'Inverno e Luck, 2001). Come evidenziato dagli esempi sopra esaminati, non vi è alcuna necessità che siano installati direttamente sul computer di un sospetto. Questo causa molti potenziali problemi. Ad esempio, un trojan tedesco può fare dei resoconti su un sospetto tedesco, anche se lui (e il suo computer portatile) si trovi all'estero (problema di territorialità), e il trojan può migrare attraverso le piattaforme (problema della specificità dei mandati ecc.).
Inoltre, essi sono (semi) autonomi. Questo può potenzialmente causare una serie di problemi. Ad esempio, in Germania la legge prevede delle conseguenze giuridiche a stati mentali rilevanti degli agenti di polizia o pubblici ministeri. Le leggi tedesche che regolano i poteri della polizia spesso fanno uso di un vocaboli che esprimono una "gradazione" nell'attribuire responsabilità ed autorizzazioni per gli ufficiali di polizia umani. Un tipico esempio è il concetto di Anfangsverdacht "avendo un iniziale sospetto" (§ § 152, 160 StPO) che fa scattare il fermo e la perquisizione. Di conseguenza, se la RFS sostituisce un essere umano e può agire con un certo grado di autonomia, la nozione di Anfangsverdacht dovrebbe essere applicata a programmi software.
Inoltre, poiché questi strumenti possono lavorare in modo autonomo, senza l'intervento diretto di una persona responsabile, la loro ricerca non è limitata ad uno specifico periodo di tempo. Di conseguenza, esse sono (potenzialmente) onnipresenti e "always on". Questo mette in pericolo l'equilibrio tra la privacy e gli interessi di Stato che, per esempio, la legislazione attuale delle prove cerca di bilanciare, e sfuma i confini tra la sorveglianza preventiva e di indagine diretta per un reato. La realtà presunta dalle vigenti leggi sulla privacy in una società liberale è un mondo in cui la "norma" è l'assenza di interferenze da parte dello Stato, a meno che le condizioni ben definite inneschino un potere da parte dello Stato di "intrusione" in questa sfera privata. È discutibile se almeno questo abbia ancora senso in un ambiente in cui abbiamo costantemente trasmissione di informazioni private al mondo, e le condizioni di attivazione si limitano a disciplinare la misura in cui queste informazioni possono essere intercettate.
Questo inoltre attenua i confini tra pubblico e privato, se si pensa a come tecnologie simili siano usate anche (legittimamente e illegittimamente) da organizzazioni private. Potenzialmente le stesse tecnologie che proteggono gli utenti da veri malware sarebbero anche efficaci contro l'operato dei RFT della polizia, sollevando la questione dei confini dell' "autodifesa" contro legittime attività di polizia.

4. Problemi

L'ultimo paragrafo ha messo in evidenza che la progettazione di questi nuovi strumenti d'indagine solleva una serie di problemi. Questi problemi possono essere generalmente suddivisi in due gruppi. Il primo gruppo è quello dei problemi connessi con l'uso della tecnologia. Questi possono essere suddivisi problemi tecnici e giuridici. Ai fini di questo articolo, l'attenzione sarà concentrata su problemi tecnici, con solo un breve sguardo su i problemi giuridici.
Il secondo gruppo sono i problemi connessi con l'uso dei dati raccolti da tali dispositivi di indagine. Ancora una volta, questi possono essere suddivisi in due sottocategorie, l'analisi dei dati ottenuti e l'utilizzo dei dati a fini di prova in un procedimento giudiziario.

4.1 Problemi tecnici

Si verificano molti e grossi problemi quando si utilizzano strumenti RFS nelle indagini di criminalità, ed è stato messo in discussione alla radice quanto questo utilizzo sia tecnicamente fattibile (Buermeyer, 2007). E certo è che non tutti i problemi possono essere citati in questo articolo. Di seguito, si sintetizzano i problemi più urgenti.
Il primo serio ostacolo tecnico da superare è l'implementazione del RFS sul sistema preso di mira. Le diverse opzioni di infiltrazione sono state delineate in precedenza (vedi punto 3.1). Il problema col quale le autorità si confrontano relativamente ad ognuna delle opzioni indicate è l'elusione da parte di prodotti anti-virus. In sostanza, un trojan federale, virus o rootkit è, da una prospettiva di progettazione, nient'altro che un pezzo di malware. Come Hilley sottolinea, "più di 200000 diversi esempi di virus, worm, trojan, spyware e adware vengono già rilevati da prodotti per la sicurezza, e questi prodotti anti-virus si perfezionano sempre di più nella loro ricerca di malware inedito '(Hilley, 2007). Questi prodotti sono progettati per rilevare qualsiasi software che sembra essere nocivo e mira ad ottenere l'accesso non autorizzato a un computer. Il problema è che ogni RFS progettato dal governo come strumento di indagine ha tali caratteristiche e attributi e può quindi essere rilevato da prodotti anti-virus perché questi non sono in grado di distinguere tra un "trojan federale" e un trojan "maligno". Il rischio se il trojan viene scoperto, come Casey e Stanley sottolineano, è che gli indagati nell'ambito dell'inchiesta possono accorgersi dell'attività investigativa e osservare o sovvertire la comunicazione con il sistema remoto (Casey e Stanley, 2004). Inoltre, se rilevato dal sistema di anti-virus, gli indagati potrebbero fare una copia dello strumento RFS e utilizzarlo per spiare le altre persone.
Una possibile soluzione per l'individuazione da prodotti anti-virus potrebbe essere la collaborazione con fornitori di software di sicurezza. Le autorità dovrebbero chiedere a questi di fare in modo di non rilevare gli RFS. Tuttavia, i clienti

acquistano tali prodotti per la protezione da eventuali malware che tenta di infiltrarsi nel sistema. Pertanto, se i produttori di software di sicurezza fossero d'accordo a collaborare con le autorità per non selezionare il software governativo, il rischio però sarebbe che i consumatori perdano fiducia nei prodotti che comprano. Il consulente di sicurezza Graham Cluley della Sophos anti-virus dice che se un cliente inoltra un trojan sospettando che sia utilizzato per spiarlo, loro gli assicureranno una protezione. Egli sostiene che è impossibile stabilire se per l'utente il software è stato progettato da parte delle autorità, e anche in caso affermativo, se è stato effettivamente utilizzato per indagare su un sospetto, o se è stato dirottato da un terzo (Hilley, 2007). Decisamente non individuare il software governativo significa creare una lacuna nella sicurezza nel software anti-virus. Questo potrebbe essere sfruttato per infiltrare i computer con malware non governativo.

Inoltre, le aziende che forniscono software anti-virus non sono necessariamente nella stessa giurisdizione come il sospetto in questione. L'incentivo per una società statunitense a cooperare con la polizia tedesca, a scapito dei suoi clienti, è minimo. Di qui possono entrare in contrasto con le rispettive leggi sulla privacy. Ancor più difficile sarebbe la regolazione di strumenti anti-virus basati sull'open source, visto che sono utilizzati da una comunità "diffusa" e non da soggetti giuridici facilmente identificabili. La questione è chi dei venditori (se non proprio nessuno?) obbedirebbe? Il governo tedesco ha quindi deciso, in questa fase, di non collaborare con venditori di software anti-virus (BT-Drucksache 16/4995).

Supponendo che lo strumento sia correttamente installato sul computer utilizzando uno dei metodi di cui sopra e dopo aver eluso con successo il software anti-virus, un ulteriore problema tecnico sta nella necessità di una connessione a Internet. Gli strumenti RFS possono accedere solo se un computer di un sospetto è collegato a Internet. Analogamente, una connessione a Internet è necessaria per trasferire indietro all' operatore i dati acquisiti. Ciò significa che se il computer è disconnesso da internet prima o durante l'inchiesta, lo strumento RFS non può essere installato con successo i dati acquisiti o non trasferito per l'operatore.

4.2 Aspetti legali

Le caratteristiche di queste tecnologie e dei relativi utilizzi possono risultare potenzialmente molto utili per le investigazioni penali, ma allo stesso tempo possono dar luogo a numerose problematiche giuridiche (Abel, 2009). In questo paragrafo, esamineremo brevemente quanto il sistema legale tedesco offre una soluzione a questa dicotomia.

Il 25 novembre del 2006 , il pubblico ministero della Corte federale tedesca, la Bundesgerichtshof (BGH), respingeva la richiesta dell'avvocato generale di perquisire il computer del sospetto utilizzando uno strumento RFS. L'avvocato generale proponeva appello contro la decisione dello BGH, affermando che gli articoli 102 , 110 e 94 del codice penale (Strafprozessordnung- StPO) consentivano di effettuare questo tipo di perquisizione. La corte fu di diverso parere e rigettò nella sentenza l'analogia fra la perquisizione tradizionale di fonti di prova fisiche e le perquisizioni occulte di un computer, incluso il traffico di Rete, attraverso un dispositivo remoto (BGH, NJW 2007, 930).

Perciò la Corte concluse che al momento non esistevano i presupposti di diritto ai sensi del codice tedesco che permettessero l'utilizzo degli strumenti RFS nelle investigazioni penali da parte degli organismi per l'applicazione della legge.

Parallelamente al dibattito a livello federale, lo stato della Nordrhein-Westfalia ha modificato la sua "legge per la protezione della costituzione" (Verfassungsschutzgesetz) il 30 Dicembre del 2006. All'articolo 5 della legge per la protezione della costituzione del Nordrhein- Westafalen (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NRW) è stato aggiunto il paragrafo 11.

Questo emendamento dava la possibilità di analizzare ed investigare in modo nascosto nella rete, specialmente l'intercettazione delle comunicazioni effettuate sulla rete e gli accessi riservati ai sistemi IT. Questo avrebbe garantito all'agenzia per la protezione della costituzione le basi legali per la ricerca online di terminali fissi o mobili sospetti. Ciononostante, è stato inoltrato presso la Corte costituzionale federale un ricorso per incostituzionalità dell'emendamento. Il Tribunale costituzionale federale il 27 febbraio 2008 ha stabilito che l'articolo 5 II paragrafo 11 era incostituzionale e perciò illegittimo. La decisione trovava fondamento in un "nuovo" diritto personale alla segretezza e inviolabilità delle informazioni contenute nei sistemi tecnologici, per la prima volta riconosciuta dalla Corte. Il Tribunale nel suo ragionamento ha dedotto questo diritto da quello inviolabile alla dignità personale e alla personalità previsto dall'art 2 I in combinato con l'articolo 1 I della Costituzione. Questo diritto può essere solo limitato, e perciò l'utilizzo delle tecnologie investigative basate su RFS da parte degli organismi per l'applicazione della legge è solo concesso laddove siano messi a repentaglio altri diritti di grado superiore come la vita e l'integrità di altri soggetti, la libertà o altri beni comuni essenziali per l'esistenza dell'essere umano. Mentre questo principio lascia aperte le porte all'utilizzo dell' RFS per la prevenzione di un imminente attacco terroristico, non può essere utilizzato per investigarne retrospettivamente uno né per la generale prevenzione di atti di terrorismo in assenza di una specifica, imminente e identificabile minaccia.

Comunque sarà necessario che un giudice ne autorizzi espressivamente l'uso su base discrezionale a seconda della circostanza concreta.

4.3 Analisi dei dati

Dato per possibile che gli strumenti di investigazione che utilizzino la tecnologia RFS siano legalmente ed utilmente impiegati dalle autorità per controllare i sospetti, la quantità di dati accumulati durante le investigazioni può rilevarsi corposa. La finalità di questi strumenti è quella di monitorare qualsiasi attività e di copiare tutti i dati e le email memorizzate sul computer del sospetto. Questo consente agli investigatori di acquisire, oltre ai documenti rilevanti, anche passwords, chiavi di crittazione e una visione approfondita delle comunicazioni intercorse.
Una delle motivazioni per usare gli strumenti RFS durante le investigazioni è quella di aumentare l'efficienza e di ridurre al contempo l'impiego di risorse umane. La raccolta di dati sarà perciò automatizzata. Questo significa che nessun soggetto umano deciderà quali saranno i dati rilevanti e che dovrebbero quindi essere copiati e trasmessi. Il problema con questo è che anche se gli strumenti RFS aumentano l'efficienza della raccolta dei dati e riducono la necessità di mano d'opera per raccoglierli allo stesso modo però possono creare problemi quando si tratta di analizzarli. Questo è il caso perché collezionano casualmente qualsiasi dato registrato sul computer o qualsiasi email inviata o ricevuta. Perciò insieme a una quantità di dati rilevanti ai fini investigativi verranno inviati anche dati irrilevanti. Allo stesso modo una quantità di dati potenzialmente problematici ed altamente sensibili, come le informazioni mediche e sanitarie o documenti equivalenti a pagine di un diario potranno essere copiate e trasmesse alle autorità investigative. Nei limiti in cui questi dati sono parte della vita privata la costituzione riconosce agli stessi una protezione specifica e perciò sono generalmente protetti dalle attività investigative. (BVerfGE 80, 367). Da questo discende che le autorità non possono analizzare ed utilizzare tali dati. In ultima istanza, i dati di questa natura che sono stati raccolti indiscriminatamente devono essere cancellati e non possono essere utilizzati a fini investigativi (BVerfGE 109, 279; 113, 348). Questo è in sé e per sé un processo molto complesso e lungo. Comunque, ancora più problematico e che la sentenza della Corte Suprema Federale ha stabilito come requisito per l'utilizzo degli strumenti RFS da parte degli organismi per l'applicazione della legge che l'affidamento del processo di selezione sia effettuato da un giudice istruttore, un procuratore di stato o da un ufficiale giudiziario (BVerfG, NJW 2008, 822). Al momento come rileva Cristoph Frank, capo dell'associazione dei giudici tedeschi, il sistema giudiziario tedesco non dispone delle risorse umane sufficienti. (Frank 2008).

4.4. Utilizzo come prova

Quando si utilizzando metodi tradizionali per l'acquisizione della prova questa viene acquisita da fonti statiche mediante un'interazione fisica. Questo significa, come Kenneally mette in rilievo, che l'acquisizione tradizionale di prove digitali riflette la natura della scena del crimine dove spazio e tempo sono ben determinati. (Kenneally, 2005) .
Tradizionalmente, quando i computers sono ispezionati durante le investigazioni per mettere al sicuro i dati importanti, il computer o l'hard disk sono presi e messi off-line per garantire che non vi siano modifiche e che l'oggetto di indagine sia nella stessa condizione quando la prova viene ammessa, così come quando il crimine ha trovato luogo. Una volta che questo processo è avvenuto i dati rilevanti vengono messi al sicuro. Dall'altra invece quando le autorità utilizzando gli strumenti RFS per ispezionare i computer e acquisire le prove questi computer vengono raggiunti da remoto, rimangono nel controllo dell'indagato e rimangono connessi alla rete prima, durante e dopo le operazioni di ispezionamento. Questo significa che non esiste una fonte fisica per fare una comparazione successiva con la prova ammessa. In altre parole, una immagine live (o copia) può essere confrontata e verificata solo con sé stessa dal momento in cui essa è stata acquisita, laddove invece immagini di macchine "morte" possono essere confrontate con i media originali" (Kenneally 2005).
Perciò il problema dell'acquisizione della prova utilizzando strumenti RFS è che non solo la fonte originaria (il computer) non è stata sottoposta a sequestro ma che questo non è neanche un ambiente statico ma flessibile, che può essere manipolato. Come regola generale la prova ricavata da network non sicuri, come Internet, può essere sempre soggetto a una sfida sulla sua autenticità e affidabilità.
Comunque, la fonte e l'ambiente non sono gli unici problemi relativi alla collezione di dati effettuati mediante strumenti di RFS. Il design dello strumento RFS, come un trojan, genera ulteriori problematiche. Casey e Stanley, che mettono in evidenza che l'utilizzo di RFS ideati senza un' infrastruttura per la preservazione delle prove è rischioso, mettono in evidenza anche questo (Casey e Stanley 2004). In via generale, come affermato sopra, i tools RFS non sono altro che malware, ideati per infiltrarsi nei computer e per raccogliere i dati. Quindi il processo è finalizzato a raccogliere i dati, non

di farlo legalmente.

Quindi, la questione è quanto i dati raccolti mediante gli strumenti di indagine RFS dovrebbero essere ammessi come prova nelle aule di giustizia. Fino ad oggi non esiste alcuna giurisprudenza in merito. In Inghilterra almeno un caso concernente l'interazione tra i trojan e la prova elettronica ha fatto un po' di chiarezza sulle problematiche legali sorte, e, sebbene il diritto processuale tedesco sia differente da quello inglese, suggerisce alcune problematiche che probabilmente potrebbero sorgere.

Il caso R vs Aaron Caffrey mette in evidenza come sia difficile risolvere i problemi legati alle nuove tecnologie all'interno di un contesto legale tradizionale (George, 2004). Caffrey era stato assolto per la violazione della sezione 3(1) del Computer Misuse Act (1990) per aver effettuato illecite modifiche a del materiale informatico, presumibilmente dopo aver acquisito illecitamente i privilegi di amministratore ai servizi Web sul computer del Port of Houston, sfruttando una vulnerabilità del software Microsoft.

Nella sua difesa ha affermato che degli hackers avevano utilizzato un trojan per impadronirsi del suo computer e che attraverso questo hanno lanciato dei programmi per hackerare il computer del Port of Houston. Sebbene non fossero state trovate sul suo pc delle tracce di un trojan e che quindi fosse altamente improbabile che degli hackers si fossero impadroniti del suo computer, Caffrey venne assolto dal reato sulla base che non potesse escludersi il fatto che un trojan si fosse installato sul proprio computer per poi autodistruggersi successivamente, non lasciando alcuna traccia.

Questo caso mette in evidenza l'incertezza del diritto quando si tratta di utilizzare questi strumenti. Mette in evidenza inoltre la difficoltà di applicare le regole tradizionali della ricerca di prova all'utilizzo degli strumenti RFS da parte degli organismi per l'applicazione della legge. Se non può essere provato che un trojan si sia installato sul computer, sarà parimenti difficile dimostrare che un trojan o un software di uguale tipologia non abbia manipolato i dati durante la fase di raccolta di dati. Problemi sostanziali almeno in Germania sembrano svilupparsi di pari passo. Come abbiamo visto la Corte costituzionale ha rigettato l'interpretazione analogica delle leggi che permettono alla polizia di effettuare fisicamente le ricerche presso l'abitazione del sospetto e ha insistito su regole nuove e sui generis regolanti il RFS. Allo stesso modo l' analoga applicazione di regole relative alla gestione, interpretazione e stoccaggio delle prove fisiche non può essere estesa analogamente alla prova raccolta con i RFS, dal momento che una delle più importanti caratteristiche della prova, ovvero l'indipendenza della prova osservata e l'osservatore, non può essere più garantita.

5 La prossima generazione di Investigatori

I progressi della tecnica hanno nel passato messo spesso alla prova i sistemi legali esistenti. La risposta del legislatore è stata spesso una soluzione studiata ad hoc. Come Casey fa notare, 'frequentemente la legislazione e la giurisdizione seguono battibeccano fra di loro, con la legislazione che risponde ad una decisione poco saggia con nuove leggi, solo per avere le corti che interpretano la nuova legislazione alla luce degli avanzamenti tecnologici' (Casey 2008). Questa legislazione "speciale" è redatta per regolare specificatamente una tecnologia. D'altra parte questo significa che un piccolo avanzamento della tecnica può causare grossi problemi di regolamentazione. La risposta della Corte Federale Tedesca in relazione agli strumenti RFS fino ad ora ha seguito questo tradizionale modello regolatorio. L'inevitabile risultato di questo approccio come evidenziato poc'anzi, è la necessità di uno scrutinio post investigativo fatto in prima battuta dal giudice investigativo ed in seconda battuta dalle corti . Perciò la domanda è se un approccio alternativo ulteriore rispetto a quello regolatorio legislativo possa regolare questi tecnologie evitando i problemi sopra menzionati.

Più promettente sembrerebbe la regolamentazione mediante il codice sorgente del programma. Il codice sorgente può essere considerato come il DNA della tecnologia. Determina la capacità di autonomia, le potenzialità e l'intelligenza della tecnologia. Perciò, se progettato in modo opportuno il codice sorgente degli strumenti RFS potrebbe permettere a queste tecnologie di funzionare in linea con la legislazione, facendo sì che questi strumenti comprendano i diritti e i limiti che si applicano alle azioni investigative, e fare loro effettuare alcuni dei ragionamenti legali descritti sopra. Questo metodo inoltre offre il potenziale per creare una nuova generazione di investigatori, in grado di rimpiazzare gli investigatori umani in alcune attività investigative.

Per realizzare il loro massimo potenziale nella lotta contro il crimine i trojan dovrebbero idealmente essere in grado di indirizzare i problemi in forza della loro progettazione (Shafer, 2006; Abel e Shafer, 2008): assicurando per esempio, che un trojan che raccoglie indiscriminatamente dati sospetti non faccia inutilmente perdere tempo alla polizia collezionando informazioni che per loro natura sarebbero inutilizzabili in un'aula di tribunale, che non esponga le forze dell'ordine a cause per violazione dei diritti umani e che allo stesso tempo utilizzi tutti i poteri addizionali garantiti alla polizia ma non esercitabili dagli agenti commerciali, come la penetrazione dei firewalls o altre manipolazione di sistemi informatici che comporterebbero una violazione della legge se commessi da un privato. Per uno specifico tipo di programmi , gli agenti autonomi, questa idea è stata già studiata ampiamente. I trojan possono essere visti come una particolare forma di

agenti autonomi e per il nostro scopo tutto ciò che si applica alla regolazione per il codice sorgente del programma allo stesso modo si può applicare ai trojan. La necessità di implementare negli agenti autonomi elementi di diritto è stato già fatto per alcune applicazioni commerciali (Hahn, Fley e Florian, 2005). Il sistema Hohfeld di diritti e doveri in particolare è stato proposto come base per il linguaggio degli agenti di comunicazione (Krogh e Herrestad, 1999).
Altri tentativi per l'implementazione della teoria Hohfeld sono stati intrapresi per l'intelligenza artificiale in seno alla comunità giuridica ma senza l'intenzione di utilizzarla con gli agenti autonomi. Il linguaggio "A-Hohfeld" di Layman Allan e l'analisi delle posizioni normative di Sergot sono stati fino ad ora gli approcci maggiormente sviluppati (Sergot 1999).
Il semplice esempio che segue può dare un'idea del possibile utilizzo del linguaggio Hohfeld per risolvere i problemi di cui abbiamo discusso. Se un trojan della polizia è penetrato nel computer di un sospetto e sta ispezionando l'hard disk per trovare dati rilevanti dovrebbe comprendere che alcuni tipi di dati sensibili e personali come quelli sanitari sono tutelati dalla costituzione e perciò devono essere considerati "inaccessibili" dalla polizia. Questo dovrebbe produrre una corrispondente "invalidità" a meno che non ci sia un "potere" più rilevante che fa venire meno i diritti costituzionali del sospetto e ne permette la violazione in via del tutto eccezionale. I termini Hofheld sono rappresentati formalmente come delle regole "if-then". La documentazione di queste condizioni dovrebbero essere parte dell'"header" del programma che l'agente esegue garantendo una esaustiva e ininterrotta documentazione delle procedure che sono state eseguite. In questo esempio il trojan dovrebbe cessare di analizzare i dati una volta che "sa" di aver acceduto a dati sensibili, protetti da norme di rango costituzionale. Conseguentemente, il Troiano deve essere in grado di eseguire dei ragionamenti in grado di annullare, applicando prima una regola generale, ma capace di sottoporre ad una revisione il risultato nel caso sorgesse una eccezione. Giovanni Sartor ha mostrato come queste relazioni legali possono essere espresse formalmente in un sistema che combina un'azione logica con una minima logica deontica utilizzando una base di concetti legali ispirati al lavoro di Hohfeld, ma intesi per gli agenti di comunicazione (Sartor, 2006).

6 Conclusione

Il trend attuale per lo sviluppo e l'utilizzo di strumenti RFS da parte delle organismi per l'applicazione della legge, come i trojan per fini investigativi, sta sottoponendo la legislazione e i concetti regolatori ad una sfida. Il tentativo di sottoporre ad una regolamentazione queste tecnologie in modo tradizionale, mediante norme, produce soluzioni ad hoc. Questo crea delle nuove ambiguità e sorge la necessità di uno scrutinio post-investigativo che rimuove alcuni dei vantaggi di queste tecnologie (come la riduzione di mano d'opera richiesta). Perciò è necessario un approccio futuro basato su dei principi che risultino applicabili all'intera classe delle tecnologie investigative. Questo può essere ottenuto creando delle tecnologie che abbiano elementi di diritto incluse nel codice sorgente del programma. Al momento la regolamentazione attraverso la legge è più avanti rispetto a quella attraverso il codice del programma. Ciononostante per utilizzare con successo queste tecnologie nel futuro questo deve cambiare presto e lo farà.